REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Service, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 13May2011	**2. REPORT TYPE** Master of Military Studies Research Paper	**3. DATES COVERED** *(From - To)* September 2010 - May 2011

4. TITLE AND SUBTITLE Cyber Warfare: "A Need for Beyond Goldwater-Nichols"	**5a. CONTRACT NUMBER** N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A
6. AUTHOR(S) Major Reginald J. Smith	**5d. PROJECT NUMBER** N/A
	5e. TASK NUMBER N/A
	5f. WORK UNIT NUMBER N/A
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068	**8. PERFORMING ORGANIZATION REPORT NUMBER** N/A
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSOR/MONITOR'S ACRONYM(S)** N/A
	11. SPONSORING/MONITORING AGENCY REPORT NUMBER N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT

Although the nature of war does not change, the inventions of art and science evolve resulting in innovations that prove most difficult for leaders and warfighters to effectively incorporate into their current operations. Cyberspace is a technological innovation that has been easily incorporated, but the problems resulting from the cross-organizational nature of the domain and the global pervasiveness of the medium were not adequately considered. Cyberspace is the medium which links all public and private agencies within the country and presents vulnerabilities that can be exploited by both state and non-state actors. Therefore, to better protect networked infrasture, mandates beyond Goldwater-Nichols must be initiated to ensure that organizations adhere to standards established and managed by a senior agency designed to improve response to possible attacks, economy of effort, and to maximize resources in a constrained environment.

15. SUBJECT TERMS
Cyberspace, SCADA systems, Scenario, Goldwater Nichols, Training, China, Vulnerabilities, Command and Control

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
			UU	27	Marine Corps University / Command and Staff College
a. REPORT Unclass	**b. ABSTRACT** Unclass	**c. THIS PAGE** Unclass			**19b. TELEPONE NUMBER (*Include area code)*** (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Cyber Warfare:
"A Need for Beyond Goldwater Nichols"

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Reginald. J. Smith

AY 2010-2011

Mentor and Oral Defense Committee Member: CHARLES D. McKENNA, Ph.D.
Approved: Charles D. McKenna
Date: 13 MAY 2011

Oral Defense Committee Member: LTCOL LORETTA L. VANDENBERG
Approved: Loretta L Vandenberg
Date: 13 MAY 2011

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENT AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATIONS FROM, ABSTRACTIONS FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

EXECUTIVE SUMMARY

Title: Cyber Warfare: "A Need for Beyond Goldwater Nichols"

Author: Major Reginald J. Smith

Thesis: The Department of Defense's ability to effectively exploit the capabilities of cyberspace will require incorporating interagency input throughout government and some private organizations, identifying the vulnerabilities within the network, and standardizing training requirements for Information Technology (IT) professionals throughout government. The level of integration, cooperation, and training necessary will require legislation beyond Goldwater Nichols in order to create organizations with the appropriate authorities to direct the necessary actions.

Discussion: Although the nature of war does not change, the inventions of art and science evolve resulting in innovations that prove most difficult for leaders and warfighters to efficiently incorporate into their current operations. Cyberspace is a technological innovation that has been easily incorporated, but the problems resulting from the cross-organizational nature of the domain and the global pervasiveness of the medium were not adequately considered. As the size and participation within the domain increases, so do the number of malicious actors who use cyberspace to conduct criminal and hostile actions. These cyber threats grow in frequency and sophistication. Each day US government and civilian networks are probed thousands of times and scanned millions of times, seeking gaps within the system which they may be capable of exploiting.

Reliance on cyberspace must be examined with a similar logic and process as reliance upon land, air, and sea lines of communications. Cyberspace is the medium that the organizations use to transmit and maintain critical information necessary to accomplish many of its daily mission requirements. Unlike all the other mediums, it is unique in that it is one that all US Government organizations use. Just as there exist avenues of approach for attack via air, land, and sea, cyberspace has a seemingly infinite number of avenues of approach to launch an attack on our communications and information infrastructure. The Department of Defense (DoD) and the Department of Homeland Security (DHS) have the primary missions to defend the country against attack of any sort, but neither organization owns or controls the communications pathways through which cyberspace exists. Because of the medium's ubiquity, an attack on the US government could be successfully launched from anywhere with Internet connectivity and neither DoD nor DHS would know about it. In order to improve overall coordination within and visibility of actions within cyberspace, a centralized coordination center is required. This coordination center will require authorization and mandates beyond what any current government agency or department holds in order to be effective.

Conclusion: The Marine Corps cannot write the strategy for implementing cyber policy, but it can continue the initiative of coordinating with other services in establishing a policy on both offensive and defensive measures that are consistent throughout DoD. As the services reflect upon history and the mind changing technological innovations of the past, steps must finally be

taken to prevent making the same mistakes. It took nearly a decade and a half after nuclear weapons were first utilized before a complex strategy for employing them or not employing them was articulated and implemented. One wonders how long it will be before a coordinated and effective cyber strategy will be in place.

TABLE OF CONTENTS

Introduction

Cyberspace is a technological innovation catapulted to the forefront of 21st century warfare. Although the nature of war does not change, the inventions of art and science evolve, resulting in innovations that prove difficult for leaders and warfighters to efficiently incorporate into their current operations.[1] The Department of Defense's (DoD's) ability to effectively exploit the capabilities of cyberspace will require mandates beyond Goldwater Nichols to incorporate interagency input throughout government and some private organizations, identify the vulnerabilities within the network, and standardize training requirements for Information Technology (IT) professionals.

America's digital infrastructure is critical to preserving our economic strength, government efficiency, and national security. Individuals, businesses and governments utilize networks to conduct day-to-day transactions, manage and control networked platforms, and transmit enormous amounts of information globally. Our technologically interconnected world presents both immense promise and potential risks.[2] As global network expansion proliferates, increases in malicious actors who utilize cyberspace as a means of conducting criminal actions grow as well. Each day US Government (USG) and civilian networks are probed thousands of times and scanned millions of times, seeking gaps within the system which may be exploited.[3]

What began as a means for scientists to share unclassified information has transformed into a vital national asset that has been referred to as the nervous system – the control system of the country.[4] DoD, along with the Department of Homeland Security (DHS), are now compelled to

[1] Michael Howard, Peter Paret, Carl Von Clausewitz: *On War*, Princeton University Press, page 75.
[2] Barack Obama, Presidential Proclamation, National Cybersecurity Awareness Month, http://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month, last accessed 22 Jan 2011.
[3] William J. Lynn III, Defending a New Domain: The Pentagon's Cyber strategy, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, last accessed 22 Jan 2011.
[4] The National Strategy to Secure Cyberspace, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf, last accessed 22 Jan 2011, page 8.

develop a means to adequately defend that system A corollary to cyber defense is DoD must also develop a means to wrest control of cyberspace from enemies in order to ensure the US and its Allies maintain access to it.

The military communications backbone consists of more than 15,000 networks, seven million users, and 7,166 major information technology programs spread across thousands of installations in over 88 countries.[5] Digital requirements will only increase as more devices are added to the Global Information Grid (GIG), the term DoD uses to describe the US military's primary network. Technologies such as radio frequency identification tags necessary to track military logistics, remote controlled drones, unmanned systems, and other wireless platforms will continue to be incorporated into the network, pushing the GIG to greater capacity, creating additional vulnerabilities that must be addressed and safeguarded. The day-to-day management of these networks, including defense and computer network operations, is supported by a workforce of around 90,000 IT professionals.[6] IT professionals are a high demand, low density profession who take years to educate and train and are a valuable resource in defending the nation's network.

Reliance on cyberspace must be examined with a similar logic as reliance upon land, air, and sea lines of communications. Cyberspace is the primary Command and Control (C2) medium that DoD utilizes to transmit and maintain critical information necessary to accomplish the majority of its daily mission requirements. Cyber-attacks are a constant threat to US networks and the DoD continuously labors to educate its own personnel to the increasing potential of attacks. Attacks against US networks have grown at an alarming rate over the past 20 years with

accessed 22 Jan 2011, page 8.

[5] Ibid.

[6] William J. Lynn III, Defending a New Domain: The Pentagon's Cyber strategy, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, last accessed 22 Jan 2010.

one IT official stating, "If gangs of foreigners broke into the Senate or Commerce Departments and carried off dozens of file cabinets there would be a crisis."[7] When cyber-attacks happen it is shrugged off as one of those computer problems that we must live with.[8]

DoD has acknowledged that the GIG experiences more than 3 million scans per day by unknown potential intruders.[9] In 2003 a series of attacks designed to copy data files was launched against DoD systems and computers belonging to DoD contractors and continued undetected for many months. [10] This series of attacks, labeled "Titan Rain," was suspected to have originated in China.[11] In 2006, a cyber-attack launched against the Naval War College prompted officials to disconnect the entire campus from the internet.[12] Incidents such as this further highlight the need for a more focused strategy for securing the GIG.

The tendency in DoD to downplay or disregard cyber-attacks changed dramatically in 2008 when DoD discovered that foreign intelligence agents had injected malicious code into the military classified and unclassified networks. The extent of the damage still remains secret, but it was the wakeup call needed to compel officials to view cyber security as a problem requiring immediate attention.[13]

Background:

The first recorded cyber-attack was an interagency, coalition operation which created timing failures within a Soviet electronic control system resulting in a catastrophic failure of the system with cascading effects. During the 1980s, through an apparent act of deception in order to

[7] Wilson, Clay Botnets, Cybercrime and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report For Congress, Order Code RL32114, page 17.
[8] Wilson, Clay, Botnets, Cybercrime and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report For Congress, Order Code RL32114, page 17.
[9] Ibid, Page 17.
[10]Wilson, Clay, Botnets, Cybercrime and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report For Congress, Order Code RL32114, Page 17.
[11] Ibid, Page 17. The attacks targeted Defense information Systems Agency (DISA), US Redstone, Arsenal, the Army, Space and Strategic Defense Installation and several computer systems critical to military logistics.
[12] Ibid, Page 17.
[13] Lynn III, William, J., Defending a New Domain: The Pentagon's Cyber strategy, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, last accessed 22 Jan 2011.

safeguard assets, the US unknowingly invented cyber warfare when intelligence officials were apprised of the Soviet Union's desire to acquire a list of technologies from the West any way possible.[14] President Reagan approved a plan to allow the Soviets to acquire the items on the list, except those items would have a series of minor errors in the design.[15] Russia had attempted to purchase commercial and industrial software that could be utilized on their networked systems to control various elements of its oil pipeline.[16]

> "Efforts to secure the software from US firms failed; therefore Russia shifted their focus to stealing the technology from a Canadian firm. With Canadian support, the CIA inserted malicious code into the software and Russian agents were successful in their attempts to steal the software that would be utilized on their oil pipeline. Initially, the software performed flawlessly, but soon started to malfunction. Before long, a pump on one end of the pipeline began to pump at maximum rate and a pump at the other end close, creating a pressure buildup that resulted in the most massive non-nuclear explosion ever recorded."[17]

The event signaled that the US had the capability to secretly insert code into software and exploited it at a time of its choosing. Equally, the initiative displayed the ability for cooperation across multiple agencies within government, partner nations, and private industry.

Following OPERATION DESERT STORM, the Chinese concluded that they could not defeat the US military by using overwhelming numbers and began reworking their strategies, investing in new technologies to deal with the "new battlefield of computers."[18] Chinese leaders understood that based upon the outcome of Desert Storm, war could no longer be conducted in ways that were familiar.[19] Winning a war against the US would require altering the military mindset in order to emerge victorious. China would utilize a strategy similar to the "multi-

[14] Clarke, Richard, A., Knake, Robert, K., Cyber War: The Next Threat To National Security and What to Do About It. Harper Collins Publishers, page 92.
[15] Ibid, Page 93.
[16] Ibid, Page 93.
[17] Ibid, Page 93.
[18] Clarke, Richard, A., Knake, Robert, K., Cyber War: The Next Threat To National Security and What to Do About It. Harper Collins Publishers, Page 49.
[19] Liang, Qiao and Xiangsui, Wang, Unrestricted Warfare, PLA Literature and Arts Publishing House Feb 1999, Page 5.

faceted war of sabotage" successfully utilized against US troops during the Vietnam War.[20] Attacks would be conducted in places not traditionally viewed as part of the battlespace and conducted by non-military individuals. China, considered the US' closest rival, has incorporated cyber warfare into its doctrine and strategy as a means of emerging victorious from an armed conflict.[21] Adapting strategies to counter this is proving difficult to the traditional warfighters with accepted definitions of combatants and non-combatants, and legal frameworks that protect their citizens' privacy.

China's cyber warriors are tasked with defense and offense in cyberspace for their nation's network, whereas the US military is only responsible for defending its military network.[22] In May, 2010 Cyber Command (CYBERCOM) was established with the mission to:

> "Plan, coordinate, integrate, synchronize, and conducts activities to: direct operations in defense of specified DoD information networks and; prepare to, and when directed, conduct full spectrum cyberspace operations in order to enable actions in all domains, ensure Allied/US freedom of action in cyberspace and deny the same to others."[23]

This point is important because in case of cyber-attacks, China has the ability to disconnect its internet from the rest of the world, thus reducing the threat of continued cyber-attacks and widespread damage to its infrastructure.[24] The US government has no such authority or capability.[25]

Supervisory Control and Data Acquisition (SCADA)

SCADA systems are the computers that monitor and regulate the operations of critical infrastructure industries (companies that manage power grids, telecommunications, water and

[20] Pike, Douglas, PAVN: People's Army of Vietnam, Presidio Press, Page 259.
[21] Clarke, Richard, A., Knake, Robert, K., Cyber War: The Next Threat To National Security and What to Do About It. Harper Collins Publishers, Page 50.
[22] Clarke, Richard, A., Knake, Robert, K., Cyber War: The Next Threat To National Security and What to Do About It. Harper Collins Publishers, Page 146.
[23] Tony Bughardt, The Launching of US CYBERCOM: Offensive Operations in Cyberspace, http://www.globalresearch.ca/index.php?context=va&aid=14186, last accessed 23 Jan 2011.
[24] Ibid, Page 146.
[25] Ibid, Page 146

early warning system in the possibility of a disaster situation.[27]

DoD maintains more than 535,000 real property assets with plant replacement assets of more than $700 billion. Each asset has or is comprised of at least one SCADA system.[28] Over the years, US strategists have conducted various war games in various organizations in order to determine weak points within the critical infrastructure, and utilized those lessons learned in order to eliminate and minimize vulnerabilities. It is important to understand that extensive efforts have been made to minimize the possibility of catastrophic failure of the National US GIG. Security of the infrastructure has been improved by adding depth, maintaining human interface, improving early warning systems, and enhancing system redundancy while also removing single points of failure within the system.[29]

SCADA systems provide an injection point that can be exploited by the enemy in an attempt to degrade US capabilities and its critical infrastructure. SCADA systems are common throughout the military, government and private industry, requiring shared focus and responsibility in protecting those systems from intrusion by hostile agents. The absence of enforceable policy mandating required network and data security standards for these systems means that priority for addressing vulnerabilities and establishing standards will vary by organization. Furthermore, economy of effort will remain fragmented with organizations across the US government and private industry duplicating efforts, wasting resources, and relearning the same lessons, because information is not being shared. Therefore, an enemy state or non-state actor that studies the organizational structure of USG agencies will seek to discover gaps within the nation's defenses that can be compromised and exploited. The mere separation of USG

http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf, Page 24.

[27] Ibid, Page 16.

[28] Tyley, Stacey S., Installations and Environment (I&E) Business Enterprise Integration, Office of Undersecretary of Defense, Page 2. Last accessed 20 March 2011.

[29] Ibid. Last accessed 20 March 2011

the nation's defenses that can be compromised and exploited. The mere separation of USG agencies may be an area that attackers may seek to exploit because of the potential time lag between multiple organizations with no existing protocols for coordinating critical issues.

Scenario

The following scenario provides a picture of the types of attacks that can be employed against a military unit and the implications for support that extend beyond the Armed Services' or DoD's capabilities to counter China's tactics in prosecuting a war advocates taking advantage of known weaknesses and attacking the enemy through nontraditional means.[30] Warfighting teaches to attack gaps in the enemy's defenses and Chinese planners propose a strategy of utilizing nontraditional targets (e.g. civilians, banks, media, legal) as a means of bending nations to its will.

Consider a Marine unit that is conducting pre-deployment training when a small percentage of junior enlisted Marines begin to experience financial hardships due to credit card fraud, identity theft, or questionable expenditures. Those Marines are frequently deemed more irresponsible and are frequently replaced on the deployment roster by individuals not currently experiencing financial troubles. As deployment nears, more reports of Marines experiencing the same problems continue to arise. Some of them have even been highlighted as conducting online purchases of items that have been utilized in robberies and other malicious acts. Key volunteers complain about growing concerns with spouses deploying while their families are experiencing hardships that they do not understand.

Attacks on individual military personnel in areas regarding credit, banking, mortgages or other personal areas are not considered an attack against the military or the US government and

[30] Clarke, Richard, A., Knake, Robert, K., Cyber War: The Next Threat To National Security and What to Do About It. Harper Collins Publishers, Page 51

can easily go unnoticed or unchallenged for long periods of time. Attacks on military personnel can be coordinated and focused in such a manner that they can potentially impact a unit's readiness. DoD has established policy for handling Personally Identifiable Information (PII) and provides training, but once that information has been received by individuals with nefarious intentions, there are no guidelines or policies established detailing the appropriate courses of action to repair the damage. Resolving problems of this nature requires each individual military member to work with a number of private companies (e.g., bank, credit reporting firms), federal and civilian agencies. DoD writ large cannot intervene on the individuals' behalf to protect the individuals' identities; the USMC and DoD have no authority to do so.

Vulnerabilities and the Need for Expansion of the Goldwater-Nichols Act

The above scenario is currently treated as cybercrime, which is defined as any type of illegal activity that makes use of the internet. Because of that definition, individuals potentially guilty of online terrorist or criminal activities are not within military jurisdiction to investigate. Interagency cooperation, specifically law enforcement, provides the additional layer to tie many illegal activities of internet crimes to groups committing acts of terrorism against the US. Intelligence reports have proven that cybercriminals have made alliances with drug traffickers in Afghanistan, the Middle East and other places where illegal drugs fund or other profitable activities such as credit card theft, and are used to support terrorist groups.[31] Tying drugs to cybercriminals provides additional leverage in identifying how insurgents are being funded and are able to purchase weapons and other equipment that will be utilized against American forces operating within theaters of operation, like Iraq or Afghanistan. Due to this occurrence, DoD is compelled to work closely with more non-DoD agencies than in previous wars. The

[31] Clay Wilson, Botnets, Cybercrime and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report For Congress, Order Code RL32114, Page 19.

relationships are situational and personality dependent and can easily be jeopardized during the transition of units and personnel.

More of the US economy is connected to the internet than any other nation. Of the primary civilian infrastructure sectors identified as critical by the Department of Homeland Security, all are reliant upon the internet for their basic functions.[32] Civilian infrastructure, such as, Chemical, Energy, Commercial, Nuclear, and Dams, are just a few of the sectors that utilize the internet to conduct business and are at risk. Collectively, vulnerabilities exists which affect every facet of the USG and any opening that can be exploited by potential attackers has the potential of affecting organizations throughout the network.

Current US network management is similar to the mechanics of the German war machine during the 1940s. US networks are controlled by owning organizations (Government, Military, Public organizations) and each has established measures to defend against attacks. Over time the infiltration of defenses within one organization paves the way for attacks against the next organization. During WWII, one could readily observe the precision with which the Germans would systematically destroy their opponents on the battlefield. Watching how they would adapt to changes made by the Allies, and emerge from those engagements still effective was truly impressive. Units were able to continue fighting long after their command structure had been destroyed, even up to the very end of the war. They could continue to function because of how they were structured. Tactically, the Germans were an efficient force, but strategically they were inefficient and that is what ultimately led to their defeat. Tactically, DoD is initiating measures to defend the network, but continues to overlook the need to ensure that measures are implemented which take into account non-governmental and non-military entities. The greatest vulnerability that confronts the nation in terms of cyberspace lies not in what the enemy has the

[32] Clarke, Richard, A., Knake, Robert K., Cyber War: The Next Threat to National Security, Harper Collins Publishers, Page 145.

ability to do, but network vulnerabilities that exist due to gaps created as a result of organizations functioning in isolation from others. Vulnerabilities in banking, law enforcement, higher education, information technology, and telecommunications have the potential of causing widespread damage to our infrastructure and these areas must be considered throughout government as targets of opportunity. A more prescriptive process directing agencies, companies, and units to fix these vulnerabilities is required.

Initiating a Command and Control (C2) structure resulting in a single entity that has the authority to establish and maintain standards in regards to equipment, information sharing, training, and security is a necessity in cross-leveling cyber-security into the Nation's overall security strategy. This fundamental development will improve coordination between government and private industry in regards to determining appropriate capability of systems utilized, faster notification of possible network attacks, broader training opportunities, sharing of industry lessons learned, and an integrated security plan that supports both government and civilian infrastructure.

There are a number of means through which cyber-attacks can be conducted against a nation and those attacks do not necessarily require destroying information or rendering networks useless. Attacks may be utilized as a means of denying service, altering information, or as a means of disseminating information to the population. Cyber attacks do not need to be conducted exclusively against a nation's government or military in order to damage morale or impact the public's trust in its government's ability to ensure that appropriate measures are in place which safeguard civilian infrastructure that provide access to internet based services. Attacks against public and government infrastructure have been documented and point to the need for a Command and Control entity that has the authority to rapidly implement countermeasures necessary to maintain network integrity, ensure access to reliable information, and minimize damage.

Distributed Denial of Service (DDoS) attacks are designed to flood targeted systems with messages in order to shut down that system, thereby denying service to its intended users.[33] DDoS attacks were conducted against Burma (November 2010) prior to its first election in 20 years, The Republic of Georgia (August 2008) prior to Russian military operations into Georgia and against various organizations within Estonia (April 2007). Attacks were conducted against both government and private institutions of each nation, affecting organizations to include government ministries, banks, newspapers, and broadcast agencies. Although, attacks were against separate agencies, each agency was a link in the overall communications infrastructure resulting in failed access to public and private institutions.

The effect of the attack reduced the availability of accurate information provided to the population of Burma and also information available to agencies outside of the country.[34] The Republic of Georgia's Internet service providers were unable to provide services to its customers for several days, therefore, communication between the government ministries, internal websites providing information to the public, and to the international community was severed.[35] DDoS attacks in the case of Estonia were similar to those of Burma and Georgia, but can be considered to have had a greater impact because Estonia has a greater reliance upon internet services than the others. 72.3% of the Estonian population utilizes internet services on a daily basis compared to less than 35 % of the previous two nations.[36] This fact is important because it illustrates how

[33] McDowell, Mindi, Understanding Denial of Services, http://www.us-cert.gov/cas/tips/ST04-015.html, Last Accessed 30 April 2011

[34] Committee to Protect Journalists, Attacks on the Press 2010 - Burma, 15 February 2011, available at: http://www.unhcr.org/refworld/docid/4d5b95d6c.html, accessed 21 February 2011.

[35] Tikk, Eneken, Cyber-Attacks Against Georgia: Legal Lessons Identified, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, Last Accessed 30 April 2011, Page 16.

[36] Internet Users Per 100 People, World Development Indicators,

quickly the problem is compounded within the population and provides insight into its effects within digitally oriented populations. Consider the effects of this type of attack when the population attempted to pay bills online or to make banking transactions. The lack of availability of core services has a huge psychological effect on the population in regards to the belief in the effectiveness, the strength, and preparedness of its government.

According to data traffic analysis, the origins of DDoS attacks can be globally sourced, suggesting a "Botnet (or multiple botnets)" and the use of exploit tools.[37] A botnet is a group of computers coupled within a domain by use of malicious code that was either knowingly or unknowingly downloaded by the users. Some of the botnets utilized during attacks against each country were from "DDoS for hire" or "DDoS for Extortion" services.[38] Utilization of services of this type assists in masking the country responsible for attacks. Establishment of a single C2 element would improve the amount of time that it takes knowledge of an attack to be relayed to Systems Managers and measures to be implemented to defeat the attack.

Exploit Tools are an inexpensive means of acquiring information for computer vulnerabilities and later listing those services for sale online in hacker's black market.[39] Lists detailing addresses of computers that have been infected with spyware and are waiting to be remotely controlled as part of a "Botnet" are readily accessible.[40] Further investigation show evidence that attempts were made to conduct a cyber-blockade against the Republic of Georgia's network and to redirect all traffic through Russia.[41] According to various sources, there were some

http://data.worldbank.org/indicator/IT.NET.USER.P2, Last Accessed 30 April 2011.

[37] Tikk, Eneken, Cyber-Attacks Against Georgia: Legal Lessons Identified, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, Last Accessed 30 April 2011, Page 13.

[38] Ibid, Page 13.

[39] Wilson, Clay, Botnets, Cybercrime and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report For Congress, Order Code RL32114, Page 21.

[40] Ibid, Page 21.

[41] Tikk, Eneken, Cyber-Attacks Against Georgia: Legal Lessons Identified, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, Last Accessed 30 April 2011, Page 12.

attacked websites that remained online and made little to no changes to defend themselves.[42] A few made changes and ultimately, many resorted to establishing blogs to pass information or relocated their sites to another country.[43] A proven attack on servers within one country by another could be considered a hostile act by the country which hosts the servers. In the case of each country, there were no established procedures or single source that could readily provide guidance throughout the public and private sector.

It is necessary to point out that, although defensive measures are more robust and a greater probability to defeating attacks against its networks exists, the US is vulnerable to attacks similar to those prosecuted against each of the above nations. Evidence of a cyber-blockade is revealed when in various reports which reveal that 15 percent of the world's internet traffic including data from the Pentagon and other government websites was redirected into China.[44] The redirection occurred for a period of about 18 minutes.[45] A research scientist at the Georgia Tech Research Institute (United States) stated that incidents where large amounts of information are routed through multiple nations occur two to three times per year.[46]

Statistics show that 78.1 percent of Americans have daily access to the World Wide Web (WWW).[47] DDoS attacks against organizations that provide access to services for conducting daily business transactions, or services that support access to information for long periods of time has the potential to negatively impact public sentiment if it is discovered that adequate measures were not initiated to protect the network from known threats. The methods employed

[42] Tikk, Eneken, Cyber-Attacks Against Georgia: Legal Lessons Identified, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf, Last Accessed 30 April 2011, Page 15.
[43] Ibid, Page 15.
[44] Miller, Joshua Rhett, Internet Traffic From US Government Websites was Redirected Via Chinese Networks, http://www.foxnews.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers/, Last Accessed 30 April 2011.
[45] Ibid
[46] Ibid
[47] Internet Users Per 100 People, World Development Indicators, http://data.worldbank.org/indicator/IT.NET.USER.P2

by groups or nations in regards to cyber-attacks will vary, but the authority to implement countermeasures across both government and private organizations must not be.

DoD's information security branch established policy mandating that each Service train and prepare IT professionals to ensure, the integrity, authenticity of information, and to protect the confidentiality of each computer within the GIG. Protecting each computer is similar to a Battalion Commander attempting to protect a fifty mile front. He tries to protect the entire front and discovers that he does not possess the capability to rapidly project power to any specific position at the time it is most required. Networks must be separated into nodes and strategically located in order to ensure redundancy and to ensure network integrity in case of attack. If the primary nodes suffer failure due to an attack, the backup will become the primary with minimal network interruption.

The proliferation of technology has rapidly blurred the lines between what lies within military or civilian jurisdiction. More and more military operations are inclusive of civilian agencies due to operational requirements, skill sets, knowledge base and access to additional resources. In order to effectively protect the nation's critical infrastructure it is imperative that policy be implemented mandating military-civilian cooperation. While interagency cooperation is improving, relationships are often established ad hoc, and personality conflicts can sometimes derail some operations causing unnecessary difficulties.

Recent history of modern warfare has reinforced the reality that success can only be obtained through the coordinated efforts of the whole of government. Wars in both Iraq and Afghanistan provide insight into the necessity of military, multiple government and civilian organizations operating in concert to align multifarious, and seemingly unrelated, lines of operations in order to accomplish America's desired end state. The openness and fractured control of cyberspace mandates that some issues will not be resolved solely through military means. Measures must be undertaken throughout government in order to leverage efforts, experience, and ideas in regards to securing the Nation's nervous system. Mutual support and cooperation across organizational lines leverages the capabilities of IT professionals and provides additional depth in defending US computer networks. This can only happen if the Goldwater-Nichols Act of 1986 is expanded to include non DoD governmental agencies in order to maximize economy of efforts, information sharing, establish agreed upon terminologies, and develop a means to incorporate technical training for military and civilian IT professionals.

Establishing a viable C2 structure and creating publications that focuses on terminologies that can be readily understood throughout government, military and private enterprise will prove advantageous. Guidelines must be established similar to those found in joint publications establishing a guide disclosing terminologies and their definition for the Uniformed Services. The same thing needs to take place within the intergovernmental agencies and the military. Considering the problems that services experience with terminology when Goldwater-Nichols mandated they work under the same umbrella. Standardizing terminologies with respect to cyber can resolve many issues in regards to language barriers and requirements to establish terms and definitions prior to the start of any necessary planning. Standardizing terminology across organizations improves the probability that everyone at the table understands the desired starting point and the desired end state.

Training:

In 2004, DoD established Directive 8570.1 mandating Information security training, certification and workforce management. The Directive required that all DoD information security technicians and managers be trained and certified to defend DoD information,

information systems and information infrastructure.[48]

Following the publication of the Directive, each Service embarked upon a strategy to train and educate its IT workforce in order to ensure that they were in compliance with the mandate. Training provided to IT professionals was in compliance with the interpretation of the Services and not according to a sole entity. An Army leader stated, "We have no doctrine at this point as to what the cyber warfighting domain is and we're training in a way that's different from the way we're fighting.[49] The Air Force has begun an undergraduate course provides its graduates with the fundamental training to establish, secure, operate, assess and actively defend seven types of networks, including command and control systems, IP, telephony, satellite and mobile telecommunications.[50]

According to orders, Navy and Marine Corps deputy CIOs must ensure that their respective information security workforces comply with identification, training and certification requirements.[51] The preceding training information illustrates how diverse training is across the services and further details the amount of energy and resources that is lost as a result of a disconnected training strategy. If one were to review training initiatives across other federal agencies, it is a fair estimate to conclude that similar training strategies are being conducted throughout government.

Cyberspace is not solely a means of transmitting data, but also an avenue of approach that can be exploited by the enemy. IT professionals must be trained to continuously monitor the

[48] Department of Defense Directive, Number 8570.01, August 15, 2004, Certified current as of Apr 2007, http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf, Last accessed 20 March 2011.
[49] Corrine, Amber, Army CyberCom Faces Tough Challenges Getting Started, http://www.defensesystems.com/Articles/2010/12/09/Army-IT-Day-Keynote-Cyber-Command-Challenges.aspx, Last Accessed 20 March 2011.
[50] Griggs, Susan, New Officer Course Boosts Cyberspace Transition, http://www.af.mil/news/story.asp?id=123210464, Last Accessed 20 March 2011.
[51] Corrine, Amber, Navy Tightens Cybersecurity Training Rules, http://gcn.com/articles/2010/07/14/navy-cybersecurity-information-assurance-directive.aspx, Last Accessed 20 March 2011.

network, identifying, and improving gaps within its defenses, to remain knowledgeable of regular and irregular occurrences within the network, and to react as required to malicious activity or attacks. System administrators have incorporated data management tools to enhance their ability to detect network intrusions and other types of malicious code that may be introduced into network as another layer of defense. Although training has dramatically improved since initiation of Directive 8570.1, there remain IT professionals who have not completed required training.[52] Immediate action procedures must be implemented and continuously rehearsed until they become routine. This fundamental belief and practice must be ingrained into their psyche in order to ensure its enduring effectiveness. A transition of this magnitude is not easy and adequate training facilities are limited. Leveraging resources within DoD, government and private industry in regards to training and education is one way to maximize efficiency and increase overall effectiveness.

IT professionals must be conditioned to adapt and improvise in response to changing situations, and if provided the required tools, access and authorizations, can rapidly identify potential problem areas. Training for IT professionals must be just as effective in order to minimize reaction times and possible misinterpretation of information being processed. If an IT professional has not been exposed to a particular situation, that individual has no experience or mental history necessary to associate the event.[53] Therefore, he is unable to fully make sense of the dilemma in order to determine if there is a possible threat. Without appropriate training and conditioning, an IT professional's reaction to a situation could prove to be harmful resulting in catastrophic loss, network failure, or even physical destruction. The Mann-Gulch disaster is an

[52] Hoover, J. Nicholas, Closing the Cyber-Security in Government, http://www.informationweek.com/news/government/security/227100067, Last Accessed 30 April 2010.

[53] Choo, Wei Chun, The Knowing Organization: How Organizations Use Information To Construct Meaning, Create Knowledge, and Make Sense, Oxford University Press, Page, 5.

illustration of how decisions are made when training is not standardized and fragmented.

The Mann-Gulch disaster was a wild-fire that resulted in the deaths of 13 out of 16 firefighters during efforts to establish fire breaks ahead of an ensuing blaze.[54] The crew was a highly select group of individuals, described as professional adventurers, which consisted of men between the ages of 17-28. Seven were forestry students, and 12 had military service.[55] Each of the firefighters had received some form of training during their careers, but most had not received training that was developed, approved, and standardized by the Department of Forestry.

Mann-Gulch illustrates how a team reacted to a crisis as the situation began to disintegrate. As the firefighters were confronted with more challenges than usual, combined with the inability to make sense of the situation, they became more anxious, ultimately forgetting training and succumbing to a state of helplessness.[56] It further displays how, during times of duress, team members no longer trusted in the capabilities of the commander and each individual did what he thought was best to preserve his life. The lesson from Mann-Gulch provides a model of the negative possibilities that can develop when education and training fail to adequately prepare individuals to react and perform effectively during difficult situations.[57] Training and education that is fragmented creates a drain on resources and is also an indicator of inefficiency. Training and education must be realistic in order to provide students with references that can quickly be associated to experience and corrective measures more effectively initiated to address emerging issues. Furthermore, one also realizes that although the chain of command had been established, none of the team's personnel followed the orders of the assigned leader (when threatened with

[54] Weick, Karl E., Collapse of Sense making in an Organization, The Mann-Gulch Disaster, Administrative Science Quarterly Volume 38 (1993), page 1. Mann-Gulch occurred in the Helena National Forrest, Montana.

[55] Ibid, Page 1.

[56] Weick, Karl E., Collapse of Sensemaking in an Organization, The Mann-Gulch Disaster, Administrative Science Quarterly Volume 38 (1993), Page 6.

[57] Weick, Karl E., Collapse of Sensemaking in an Organization, The Mann-Gulch Disaster, Administrative Science Quarterly Volume 38 (1993), Page 21.

life or death) who had a better understanding of the overall situation and also possessed the key to each of their survival. Authority must be vested and everyone involved must know this fact.

Conclusion

During the modern era of warfare, success resides in uniting and utilizing the capabilities of the whole of government in order to reduce vulnerabilities, leverage resources, and share information across organizations. Technological innovations continue to stretch the limits of the perimeter, greatly impacting the personnel required in order to support military needs. Although the nature of war does not change, the inventions of art and science continue to evolve, resulting in innovations that prove most difficult for leaders and warfighters to efficiently incorporate into their current operations.[58] Cyberspace will be the venue that forces the government to finally come up with a Command and Control System that works, because this is the one element which they all share and it is going to take an act of Congress to make this happen. History has taught that determining the appropriate course of action during a crisis is the worse time to highlight that procedures must be established to protect one's assets. In each instance that a Command and Control system was not in place with established guidelines prior to an incident, the outcome was far from acceptable. Each organization undertook different courses of action and oftentimes those actions were conducted by individuals acting on their limited knowledge of the situation, failing to understand the impact from an organizational or strategic level. There are areas that require legal issues to be identified and refined, but at the end of the day, a system providing protection of the entire network and not a segment is what is required to better protect the nation.

Extending Goldwater-Nichols to include other public, government agencies and military services provides added layers of knowledge and security. There are any numbers of instances where occurrences within the civilian sector will have implications within the military sector.

[58] Howard, Michael, Paret, Peter, Carl Von Clausewitz: On War, Princeton University Press, page 75.

Due to separation, those occurrences could potentially go unnoticed for extended periods of time and soon be forgotten or undocumented because they had little or no apparent relevance. Greater coordination with other agencies also requires that agencies begin to consolidate terminology. Relationships established at this level can improve performance over the long term by enabling greater understanding of organizational culture and their practices. Building relationships is the bedrock of continued understanding of cultures within an organization.

Warfare has evolved, breaking down the distinction between military and civilian with the battlespace overlapping with non-battlespace, and serving to make the lines less clear.[59] Just think that it is even possible to start a war in a computer lab or stock exchange and send an enemy nation to its doom.[60] Thus the battlespace is omnipresent, cyber warfare, an extension of traditional warfare, provides man with the capability to conduct lethal and non-lethal operations within a virtual dimension by impacting the enemy's ability to rapidly respond to changes within his physical environment. Cyberspace provides the means to interrupt the enemy's communications, transportation, economic, and energy capabilities long before he conducts any movement of conventional forces. Modern warfare reinforces that, war is not solely a military venture and because of that fact, cyber warfare should not be relegated to that category.

There is still much that needs to be completed in order to ensure the DoD remains a force in every dimension that it conducts operations. Cyberspace has the potential to degrade capabilities to a crawl and it is everyone's responsibility to ensure there is freedom of action in the virtual dimension as well as the physical.

[59] Liang, Qiao, Xiangsui, Wang, Unrestricted Warfare, PLA Literature Arts and Publishing House, February 1999, Last Accessed 20 March 2011. Page 43.
[60] Ibid, Page 43.

BIBLIOGRAPHY

Bughardt, Tony. The Launching of US CYBERCOM: Offensive Operations in Cyberspace, (July 2009), http://www.globalresearch.ca/index.php?context=va&aid=14186.

Choo, Wei Chun. The Knowing Organization: How Organizations Use Information To Construct Meaning, Create Knowledge, and Make Sense, Oxford University Press, 5.

Clarke, Richard A., Robert K. Knake. Cyber War: The Next Threat to National Security and What to do About It, Harper Collins Publishers, 156.

Clarke, Richard A., Knake, Robert K. Cyber War: The Next Threat to National Security and What to do About It, Harper Collins Publishers, The National Strategy to Secure Cyberspace, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf, 151-155.

Committee to Protect Journalists, Attacks on the Press 2010 - Burma, 15 February 2011, available at: http://www.unhcr.org/refworld/docid/4d5b95d6c.html.

Corrine, Amber, Army CyberCom Faces Tough Challenges Getting Started, http://www.defensesystems.com/Articles/2010/12/09/Army-IT-Day-Keynote-Cyber-Command-Challenges.aspx

Corrine, Amber, Navy Tightens Cybersecurity Training Rules, http://gcn.com/articles/2010/07/14/navy-cybersecurity-information-assurance-directive.aspx

Department of Defense Directive, Number 8570.01, August 15, 2004, Certified current as of Apr 2007, http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf

Cybersecurity Current Legislation Executive Branch Initiatives, 4

Griggs, Susan, New Officer Course Boosts Cyberspace Transition, http://www.af.mil/news/story.asp?id=123210464

Hoover, J. Nicholas, Closing the Cyber-Security in Government, http://www.informationweek.com/news/government/security/227100067

Howard, Michael, Paret, Peter. Carl Von Clausewitz: On War, Princeton University Press, 75.

Liang, Qiao, Xiangsui, Wang, Unrestricted Warfare, PLA Literature Arts and Publishing House, February 1999

Lynn III, William J., Defending a New Domain: The Pentagon's Cyber strategy, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Obama, Barack, Presidential Proclamation, National Cybersecurity Awareness Month, http://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month.

Sedlacek, Elizabeth, Information Systems Infrastructure and Product Overview 2006, http://webcache.googleusercontent.com/search?q=cache:Z7YCSSHwVEsJ:www.dtic.mil/ndia/2006mcsc_apbi/sedlacek.pdf+1990+marine+corps+network&cd=8&hl=en&ct=clnk&gl=us, 12-13.

Tikk, Eneken, Cyber-Attacks Against Georgia: Legal Lessons Identified, http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

Tyley, Stacey S., Installations and Environment (I&E) Business Enterprise Integration, Office of Undersecretary of Defense.

Weick, Karl E., Collapse of Sensemaking in an Organization: The Mann-Gulch Disaster, Administrative Science Quarterly Volume 38 (1993), 21.

Wilson, Clay, Botnets, Cybercrime and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report For Congress, Order Code RL32114, 17.